ARAT BULLETIN

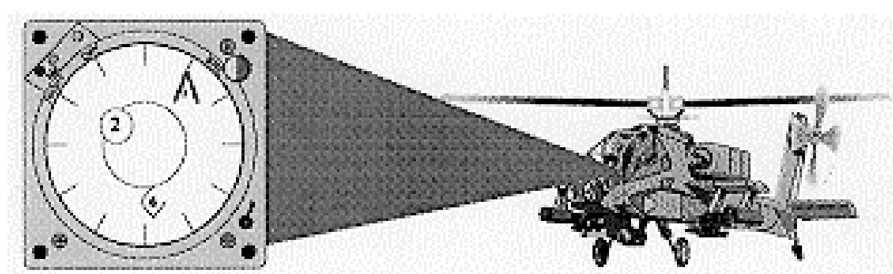
Published by ATRR-PO
Fort Monmouth, NJ 07703

Volume 2, Issue 1 **April 1995**

RADAR WARNING RECEIVERS:

MEETING THE OPERATIONAL NEEDS OF ARMY AVIATION!

What's Inside:



RADAR WARNING RECEIVERS
The AN/APR-39A (V) 1
(Part 1 in a Series)

"Our object ought to be to have a good army rather than a large one."
George Washington - 1780

The complexity of the modern battlefield, with a multiplicity of sensors on various platforms, provides an impetus for the development of passive airborne electronic warfare (EW) systems. These systems include Communications Intelligence (COMINT) and Electronics Intelligence (ELINT) systems that gather intelligence across the electromagnetic spectrum. The Army has been working this issue for a few years. One result is the AN/APR-39A (V) 1 Radar Signal Detecting Set (RSDS), an ELINT system currently coming into wide use throughout the Army.

The RSDS is designed to provide pilots with rapid detection, warning and identification of received emitter signals. Four critical features of the RSDS provide this capability. (1) It accepts and processes radar signals from threats within its system limitations. (2) The RSDS displays detected signals in a format that is readily identifiable by the air crew. (3) It provides pertinent information about the detected signals, such as direction, lethality, identity, etc. (4) Finally, it emits an audio warning to enhance the air crew's detection and identification capabilities.

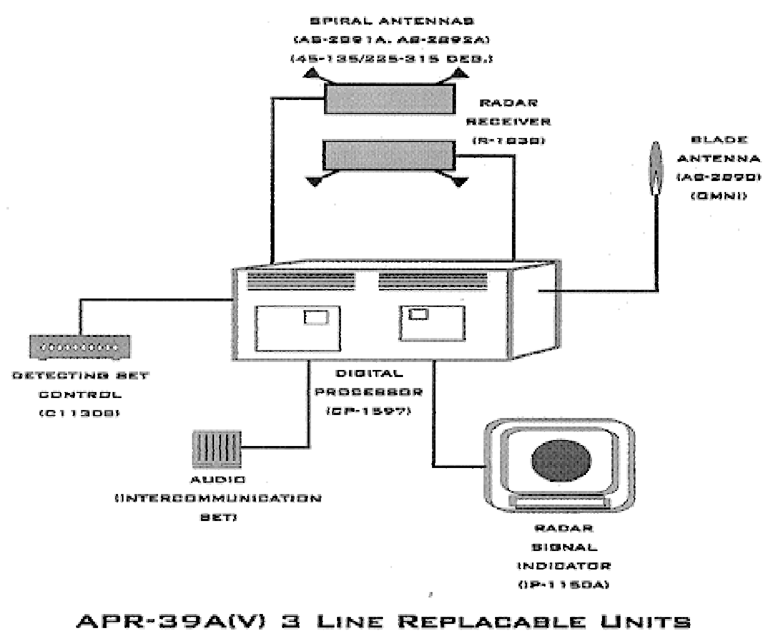


Figure 1

The AN/APR-39A (V) 1 equipment configuration consists of several different components. These include the AS-2890 Omni-directional Blade Antenna, AS-2891A and AS-2892A Direction-Finding Spiral Antennas, R-1838 Radar Receiver, CP-1597 Digital Processor, C-11308 Detecting Set Control, IP-1150A Radar Signal Indicator, and Audio Intercommunication Set (see Figure1).

RSDS provides continuous coverage for the detection and location of Radio Frequency (RF) signals in the C/D (Ultra High Frequency [UHF]) and E/J (Super High Frequency [SHF]) bands. The system provides rapid detection and display of threat radars used for fire control of antiaircraft artillery, air-to-air weapons and surface-to-air missile systems. Parameters of friendly radars may also be added to the system's stored data to aid the computer in their identification.

A series of four Direction Finding (DF) antennas (ASS-2891A & AS-2892A) and an omnidirectional blade antenna ((AS-2890) monitor the electromagnetic spectrum. These antennas divide the spectrum into low band (C/D) and high band (E/J) domains. The DF antennas pass high band signals to the High Band Quadrant Receivers (R-1838). Any accepted signals are provided to the video processor located within the CP-1597 digital processor for further analysis. Low band signals detected by the AS-2890 blade antenna pass as a single input to the C/D Band Omni receiver.

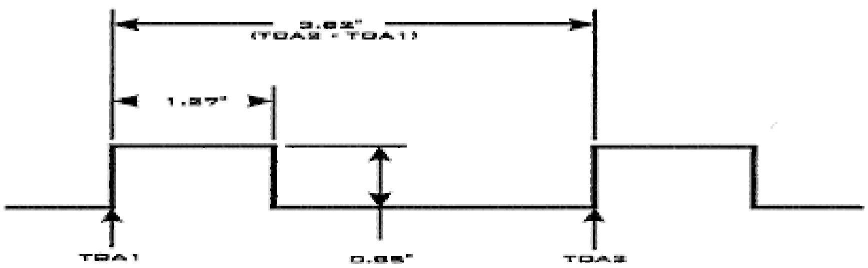
C/D band signals then go to the video processor in the CP-1597 for further analysis. Using the CP-1597 Processor for control, data is collected in each band. The CP-1597 measures each pulse for Time-of-Arrival (TOA), Pulse Width (PW) and amplitude. In the high band (E-J), the CP-1597 derives the Angle-of-Arrival (AOA) from simultaneous power measurements on

(continued next page)

AN/APR-39A (V) 1 - (continued)

the four DF antennas. Pulse Repetition Interval (PRI) is calculated between consecutive pulses (see Figure 2 for a general example).

Operating characteristics of radars normally make the situation more complicated. Amplitude of the pulses will vary over time if the radar is operating in a mode where the antenna searches the sky (SCANNING). In addition, the interval between successive pulses and the pulse width of successive pulses may not be constant. Current radars have many different PRIs, PWs, and SCAN characteristics.



RADAR PULSE TRAIN

Figure 2

The AN/APR-39A (V) 1 is a complex piece of equipment designed to provide threat emitter information quickly and accurately to aviation pilots. CECOM RDEC SEC is actively working reprogramming issues to support the AN/APR-39A (V) 1. Future articles in this series will cover such topics as systems operations, threat translation and much more. POCs are Mr. Joe Ingrao/Mr. Harinder Purewel, DSN: 992-8224.

ARAT Site Connectivity:

Establishing Secure Communications
(Part 2 in a Series)

Part 1 of this series (ARAT Site Connectivity: A WAN Approach, ARAT BULLETIN, January 1995) described ARAT-PO's approach for setting up a Wide Area Network (WAN). The WAN will connect Army Reprogramming Analysis Team (ARAT) sites in the future to quicken the exchange of information supporting Army Target Sensing System (ATSS) rapid reprogramming.

The objective of WAN concept exploration activities is to investigate, evaluate, and display possible connectivity solutions. These activities include exploitation of existing DOD and industry standard services and commonly used computer/communications components. Through this approach, a WAN solution should be attained that is cost effective, reliable and expandable.

Accessing secure data from remote sites poses three concerns: 1) guaranteed data transmission, 2) rapid access to information, and 3) maintaining appropriate levels of security. The ARAT sites use available computer resources to connect their processing equipment over common communications paths. These paths include telephone lines on the Defense Switching Network (DSN)/ commercial or the Military Network (MILNET) (part of the Defense Data Network [DDN]), which allow for direct file transfer and electronic mail. The ARAT sites have local area networks (LANs) which enable home-site computers to easily exchange collateral information. By extending this idea to a wider region, i.e., between distant ARAT sites, the connected systems become a WAN. The sending site scrambles sensitive information through use of encryption devices before transmission on common communications paths. The receiving site descrambles the transmitted information using a complimentary method.

This provides ARAT participants secure real-time electronic mail and file transfer services between remotely located engineering and support sites. For example, if an urgent message (e.g., Threat Impact Message) must be relayed to several ARAT sites, an engineer issues a broadcast mail message to a predefined set of recipients. In a matter of seconds, the message is transmitted and delivered to the appropriate electronic mailboxes across the country. Confirmation of message receipt is also available. File transfer services can be used to rapidly transmit relevant data such as mission data sets between sites.

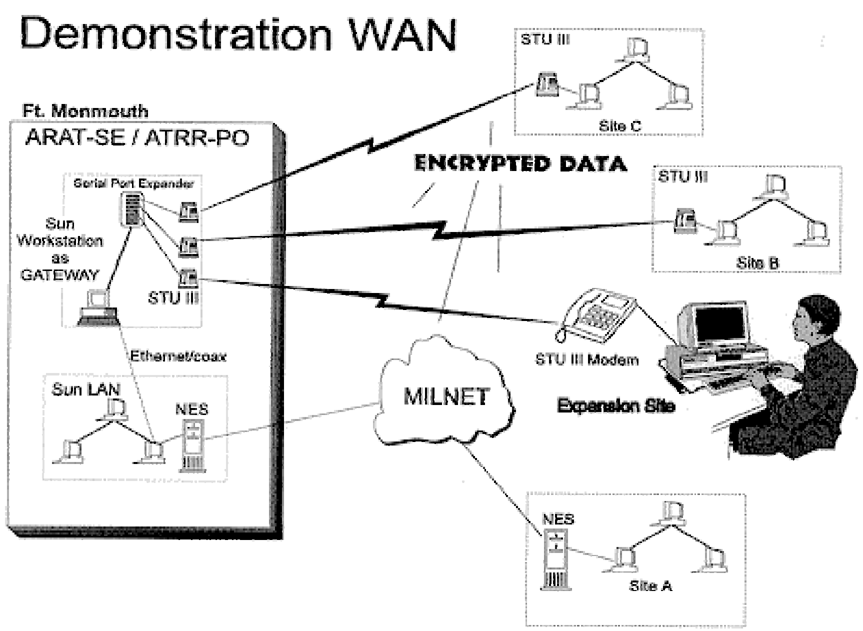
Data to be transmitted over any communications medium must be encrypted before leaving the secure facility. This is accomplished with National Security Agency (NSA) accredited encryption devices such as the

(continued next page)

ARAT Site Connectivity - (continued)

Secure Telephone Unit (STU III) for telephone transmission. A Network Encryption System (NES) can also be used which provides an interface to faster communications media such as Ethernet. The NES can be used to provide encrypted data transmission over MILNET. Newer technologies such as "Caneware" offer Multi-Level Security (MLS). Both the NES and Caneware are derived from NSA's Secure Data Network Systems (SDNS) product development.

Several ARAT sites possess Reduced Instruction Set Computer (RISC) processor-based computing equipment running the Unix operating system. These environments have been designed specifically to meet ARAT's needs in rapid processing/analysis of TSS reprogramming data. Among the reasons for ARAT sites using Unix work stations was ease of integration, and flexibility to interface with a variety of existing Army reprogramming environments. PC-compatible systems running Microsoft Windows



also play an important role in the analysis and verification phase. These systems possess the capability to communicate with each other over a wide area network.

Figure 3

Common to the Unix operating system are networking capabilities based upon the Transmission Control Protocol/Internet Protocol (TCP/IP) data communications protocols for transporting data between diverse computer systems. These protocols provide command-line control for easy access to data communications services with other work stations and hosts, either locally or remotely over packet-oriented networks. The use of a Serial Link Internet Protocol (SLIP) or Point to Point Protocol (PPP) allows the extension of these networking capabilities using standard serial (EIA-232) ports, modems, and telephone lines.

Currently, computer/ communications resources have been accredited and configured to implement secure data communications between the ARAT-PO and ARAT-TA sites. Low level E-mail and file transfer operations have been successfully displayed via phone line access with STU III encryption, and MILNET access with NES encryption. ARAT-PO intends to incorporate both transmission paths into a demonstration WAN that will provide direct connection (MILNET) and dial-up phone access for ARAT and related sites.

ARAT-PO employs an integrated approach to establishing an ARAT WAN capability. This approach includes the parallel activities of 1) analysis/design of target WAN architecture, and 2) concept exploration resulting in a demonstration WAN. Implementation of the target WAN will result from upgrading the demonstration WAN. Future articles on ARAT Site Connectivity will describe ARAT-PO efforts to set up high-level application programs designed to streamline and automate the reprogramming process. High level applications include the interactive graphical user interface for ARAT WAN work stations (e.g., World-Wide Web), remote database query, and remote application execution. POCs are Mr. Ken Kragh/Mr. Gary Conover, DSN: 992-6003.

FORT MONMOUTH TO HOLD EWIRDB CONFERENCE

CECOM RDEC SEC ARAT-PO is sponsoring the 1995 Electronic Warfare Integrated Reprogramming Data Base (EWIRDB) Conference. This conference, to be held at Fort Monmouth during 22-26 May, invites users and producers of the EWIR

(continued next page)

EWIRDB Conference - (continued)

Data Base (EWIRDB) to discuss common problems, establish future trends, and develop plans for product improvement. The following provides a short breakdown of the conference.

On 22 May, before the actual conference, Defense Intelligence Agency (DIA) will convene a management review meeting, at Fort Monmouth, limited to producer representatives and committee chairpersons. On 23 May, the first day of the conference, EWIRDB managers, producers, and committee chairpersons will present current status and plans. The morning of 24 May will be devoted to status reports on user Electronic Warfare (EW) programs, user EWIRDB requirements and recommendations. From the afternoon of 24 May through 25 May, EWIRDB committees will convene separately to address high interest issues previously specified by conferees. Findings and action plans will be presented to the full conference on 26 May, before adjournment.

Concurrent with the committee sessions on the 24th and 25th, software demonstrations, briefings, and tours will be available which highlight ARAT and EWIRDB CD-ROM capabilities. Additional information can be obtained by contacting the ARAT-PO at Fort Monmouth. POCs are Mr. Sok Kim, DSN: 992-1337/Mr. Verne Pedro, DSN: 992-6003 or DSN: 992-8198.

AN/AVR-2 & AN/AVR-2A LASER DETECTING SETS

"Difficulties is the name given to things which it is our business to overcome."
Admiral Ernest J. King: 1942

The use of laser technology for military applications is a recent occurrence. There are, currently, only a few ongoing laser countermeasures programs due to small demand. One program, for which the Army has lead service responsibility, encompasses the AN/AVR-2 and AN/AVR-2A Laser Detecting Sets (LDSs). The AN/AVR-2 is currently in full production, while the AN/AVR-2A is still under development. The primary use for the AN/AVR-2 LDS is helicopter protection, however, it is also used on fixed-wing platforms. Helicopters such as the AH-64A Apache, OH-58D Kiowa Warrior, UH-60Q Medevac, and SOA Blackhawk have received, or will receive the LDS.

LDS provides detection of laser weapons throughout a 360-degree range of coverage. Upon detection, it delivers both visual and audible warnings. LDS identifies the direction of any threat, and displays threats in a priority order of lethality. It also characterizes the type of laser, such as range finders, designators, or beamriders. Verification takes place through an interface capability with the AN/APR-39 Radar Signal Detecting Set (RSDS) family. LDS also works as a training tool by serving as a MILES/AGES Receiver.

Both the AVR-2 and AVR-2A incorporate several components together into one package. Configuration of sensor units on the AVR-2A varies. Smaller size helicopters (with the -2A(V) 1) contain 4 sensor units. Large size helicopters, such as the Chinook, (with -2A(V) 2 contain 6 sensor units. Fixed wing aircraft (with the -2A(V) 3) have 8 sensors. Thus, as the size of the aircraft increases, there is a corresponding increase in the number of sensors required to provide 360 degree coverage. All sensors feed data into the CM-493 or CM-493A (V) Interface Unit Comparator. From there, data passes to the resident AN/APR-39 (V) series RSDS for further analysis and action.

The AVR-2A emerged from the basic AVR-2 with the incorporation of several additional functions. One function allows the AVR-2A to replace the laser detection system of the MILES/AGE II training system. It also adds a User Data Module (UDM) to the Interface Unit (IFU). This provides a cost-effective means for applying either mission software or laser threat changes to the system. Another function increases Band III sensitivity and will improve threat detection performance. Inclusion of an RS-422 interface device allows for external interface with other types of RSDS besides the AN/APR-39 series. Addition of 1553B interface hooks to the AVR-2A allows for a complete internal interface on the avionics platform.

The Project Manager for Aviation Electronic (PM-AEC) has primary responsibility for acquisition of the LDS

(continued next page)

AN/AVR-2 LASER DETECTING SET
LINE REPLACEABLE UNITS

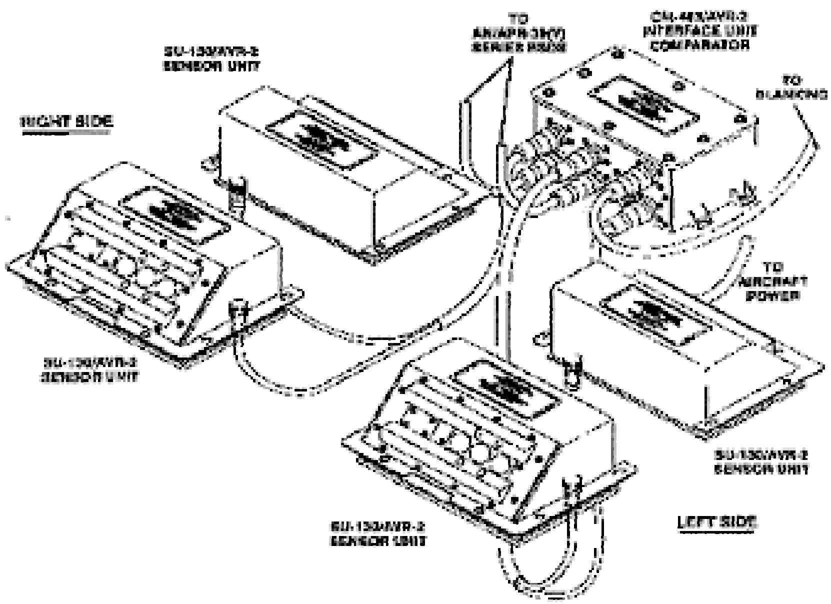


Figure 4

and its computer resources. PM-AEC also has responsibility for all maintenance issues involving the LDS. Communications-Electronics Command (CECOM) is the procuring agency for the LDS. CECOM Research, Development & Engineering Center (RDEC) Night Vision & Electronic Sensors Directorate (NVESD) is responsible for all technical issues during acquisition of the LDS and its computer resources. Software Engineering Center (SEC) provides PDSS for the LDS. SEC POC is Mr. Joe Ingrao, DSN: 992-8224.

FLAGGING: (Part 2 in a Series)

Part 1 (ARAT BULLETIN, Volume 1, Issue 2, July, 1994, provided an introduction to the process of flagging. Part 2 updates recent Army progress made in this area of concern.

During 1994, the ARAT-PO and ARAT-TA evaluated four different flagging methods in use by the Air Force. Timeliness, thoroughness and cost-effectiveness of conventional flagging methods used by Air Force Information Warfare Center (AFIWC) were compared with MAXI keyword filters at Air Warfare Center (AWC), a "beta" version of the EWJTAT parametric "out-of-bounds" flagging tool at ECSF/Air Force Special Operations Command (AFSOC), and the Selectively Improved Flagging Technique (SIFT) developed by AFIWC.

The essential conclusion of these evaluations shows the conventional flagging model as timely and reliable. In addition, this model enjoys the benefits of maturity, adequate technical sophistication and the significant infrastructure and expertise of an intelligence agency supporting flagging for many EW systems. After this period of evaluation, the ARAT-PO and ARAT-TA established routine conventional flagging support through AFIWC for the AN/APR-39A (V) 1.

ARAT-TA uses conventional flagging model outputs (flagging reports) as a key element for threat change detection and threat impact analysis. One first mission data set (MDS) has already been implemented for the Persian Gulf. A second MDS, for Korea, was tested and implemented in mid-March of 1995. Other MDS will be implemented as they become available in flagging format. The AFIWC posts flagging reports for each MDS of modeled systems to the BBS on a weekly basis, or more as needed. These reports contain an identification of the threat, parameters causing the flag, reason for the flag, and clarifying information as appropriate from the AFIWC engineer or analyst assigned to the model.

Why Perform Flagging?

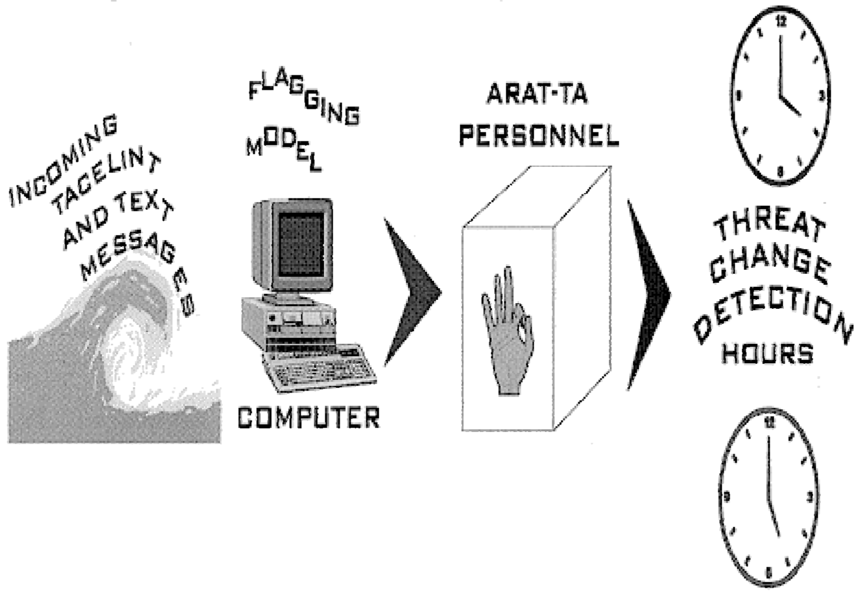
Thousands of TACELINT messages are received each day worldwide. The scope of the Army deployment does not allow a significant reduction in the worldwide view. Roughly 50,000 messages must be evaluated per month, and some estimates range higher. Threat change detection and impact analysis must be completed in a matter of hours under emergency conditions. Manual analysis of this amount simply cannot cope with this amount of data. The EW community has long recognized the need for an automated tool to parse and analyze this massive amount of intercept reports. Such a tool is essential for performance of the ARAT-TA mission (See Figure 5).

(continued next page)

Flagging - (continued)

Plans For Expanding Conventional Flagging Support

- Additional mission data sets for the AN/APR-39A (V) 1 are planned for Korea, Yugoslavia and Southern Command (SOUTHCOM). Other MDS, including the possibility of FMS MDS, may be added. The initial addition of new MDS will be coordinated by the ARAT-PO. Existing MDS may be revised from time to time. As existing MDS are updated, a simplified standard procedure will be established this way:



Flagging Tools Speed Detection Time
Figure 5

- ARAT-TA will designate a flagging directory or library within the BBS to which AFIWC and SEC have read/write privileges.

- CECOM SEC will post new and updated MDS to the flagging library. Postings will use the standard four part ASCII format required by AFIWC. These postings will occur upon AFIWC approval for release to the field.

- ARAT-TA will delete older versions of MDS, which are no longer required for flagging, from this library. ARAT-TA will notify AFIWC via email of the need to retrieve the new or updated MDS (with copy to ARAT-PO).

ARAT-TA and AFIWC will coordinate directly on geo-tailoring and other factors related to threat list development for each MDS. Such coordination allows flagging to be more accurately focused on threats and regions of interest. ARAT-TA assumes primarily responsibility for any Army-unique rules to be submitted to AFIWC for inclusion in the conventional flagging system.

ARAT-PO will coordinate with AFIWC for any changes to the conventional model. Changes can be for either parametric inputs to the model or the basic code and will be based on hardware or OFP changes to the AN/APR-39A (V) 1.

ARAT-PO will be investigating the validity for Army use of the reported AFIWC conventional model for the AN/ALQ-162 CW jammer. If suitable for Army use and cost effective, the conventional flagging agreement will be expanded to include the "Army" MDS for the AN/ALQ-162 when possible, using the same procedures as those for the AN/APR-39A (V) 1.

ARAT-PO will coordinate the development of conventional flagging models for the AN/APR-39A (V) 2 and AN/ALQ-136 (V) 2 as required. Although the full PDSS process may not be in place presently within SEC for these systems, ARAT-PO can immediately support the threat analysis and flagging aspects through ARAT-TA. Other systems now in development will also need flagging support in the future, for example, ATRJ. Future articles will continue to chronicle the progress made in the flagging area. POCs are Mr. Norm Svarrer/Mr. Phil Miner, DSN: 872-8899.

JC2WC TRAINING COURSE

The Land Information Warfare Activity (LIWA) and the Army (Target Sensing Systems) Rapid Reprogramming Project Office (ARAT-PO) recently co-sponsored a five day training course at Headquarters (HQ), Intelligence and Security Command (INSCOM), Fort Belvoir, VA. This course, titled the Armed Forces Staff College "Introduction to Joint

(continued next page)

JC2WC Training - (continued)

Command and Control Warfare Course (JC2WC)", was held from 8 Jan 95 through 13 Jan 95. Its primary purpose was to introduce the student to the evolution of Command and Control Warfare (C2W), to include key definitions of new terms, policy, doctrine, concepts, and publications.

The idea of C2W is as old as warfare itself, but the developing strategies and tactics for applying C2W are new and emerging. Operation DESERT STORM was the primary catalyst for Army senior leadership to see the importance of integrating those elements that comprise C2W in a synergistic manner. C2W is the integrated use of five elements: Operations security (OPSEC), psychological operations (PSYOP), electronic warfare (EW), military deception and physical destruction. These are mutually supported by intelligence to deny information to influence, degrade, or destroy the adversary's command and control (C2) capabilities while protecting friendly C2 against such actions.

ARAT-PO periodically sponsors or helps in sponsoring training courses that can benefit the Army and the joint services reprogramming community. More information on the JC2WC Course can be obtained by contacting the LIWA.

1/95 JC2WC Class includes representatives from all service branches

MULTI-SERVICE ELECTRONIC WARFARE REPROGRAMMING

Pick up any defense-related publication today, and you are very likely to see an article on jointness (deals with more than one military branch). Such articles are now quite commonplace. Within the realm of jointness, the issue of Electronic Warfare (EW) systems reprogramming optimization has become a critical concern. The United States Air Force (USAF) Air Warfare Center commissioned a study effort, approximately one year ago, to examine processes employed by the military services to reprogram Aviation EW systems.

Surveys were conducted at several reprogramming centers and supporting threat analysis activities within each service branch. For the Army, surveys were conducted at the Army Reprogramming Analysis Team (ARAT) Threat Analysis Center, Eglin AFB and the CECOM Software Engineering Center (SEC) Ft. Monmouth NJ. After reviewing the strengths of each service process, the study recommended process enhancements that could, or should, be carried out.

These recommendations have been presented to a Multi-Service Steering Group for consideration. Some recommendations were not accepted by the steering group due to a lack of substantive justification. Additional recommendations are being addressed by service lead working groups, many of which can be done at small cost. A short synopsis follows on these recommendations.

COMMUNICATIONS

Currently, the services employ as many as thirteen separate messages to convey reprogramming data between activities. Many messages contain similar data and some use standard formats. However, standardization between services is virtually nonexistent. Efforts are underway to standardize service distribution lists, message formats and reduce the number of messages by 50%.

(continued next page)

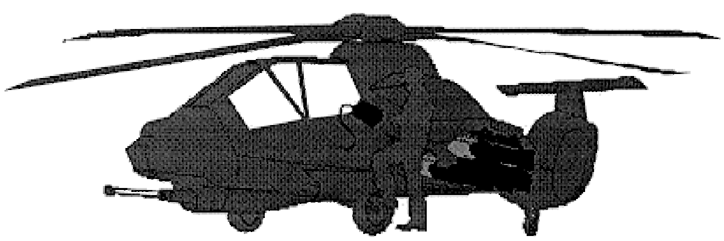
Multi-Service Reprogramming (continued)

DATABASE TOOLS

The number of database management tools in use or development is rapidly approaching the number of messages used. Tools are quite costly to develop and maintain. A tool requirements' subcommittee is being established to consolidate database management tools requirements across the services. This consolidation will include threat analysis and mission data structuring.

MEMORY LOADER VERIFIER

Apparently each platform or EW subsystem requires unique MLV support. Consequently, DOD has acquired a considerable arsenal of MLVs, largely incompatible, over time. Each of these systems requires unique training, logistics support and maintenance. The Joint Coordinating Group - EW, which reports to the service logistics commanders, has chartered a subgroup to try and standardize a family of MLVs for multi-service use.



The Army is evaluating several MLVs for possible use with helicopters.

WIDE AREA NETWORK

All three services have stated requirements to net their respective reprogramming activities. The steering group agreed to design a single WAN that interconnects all service reprogramming activities. This initiative should add efficiency to reprogramming at significantly reduced costs.

None of these recommendations will be carried out over night but collectively they represent a giant step in the right direction. Imagine this: Army helicopters embarked on Navy ships are properly reprogrammed; life cycle costs of MLVs are reduced in half based on standardization; or possessing the operational capability to reprogram land based F-18s with the same support equipment used by F-16s stationed at the same base. We are not there yet, but we are headed in the proper direction and that direction is multi-service cooperation. POCs are Mr. Norm Svarrer, DSN: 872-8899/CPT Clements, DSN: 872-2166.

To receive this publication, submit the following:

- ***Organization**
- ***POC**
- ***Address**
- ***Phone #/Fax #**

Fax to:

(908) 532-5238(U)
DSN: 992-5238(U)

or send via E-mail to:

arat@ccmail.sed.monmouth.army.mil

"ARAT BULLETIN" will be published quarterly and is intended to provide the ARAT community with current information. You are invited to submit input for improving this publication, or present articles which will be of interest to our readers. You may fax correspondence to the Editor at (908) 532-5238. Include your name, telephone number, and source of information.

... MEET THE ARAT BULLETIN STAFF...

Publishers:
Cenap Dada, Chief, A/IEW
John Hakim, Chief, CM

Executive Editor:
Sok Kim, ATRR-PO

Editor:
Ray Johnson

Assistant Editor:
Jacki Yamello